(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11515 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/14603

(22) International Filing Date: 30 May 2000 (30.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/136,714 28 May 1999 (28.05.1999) US

(71) Applicant: SPENDCASH.COM, INC. [US/US]; Suite 1401, 90 William Street, New York, NY 10038 (US).

(72) Inventors: DOHERTY, Charles, S.; 725 Miller Avenue, #429, Freeport, NY 11520 (US). TSIOUNIS, Yiannis, S.; 81 Greene Street, 2nd Floor, New York, NY 10012 (US).

(74) Agents: GARRETT, Arthur, S. et al.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US).

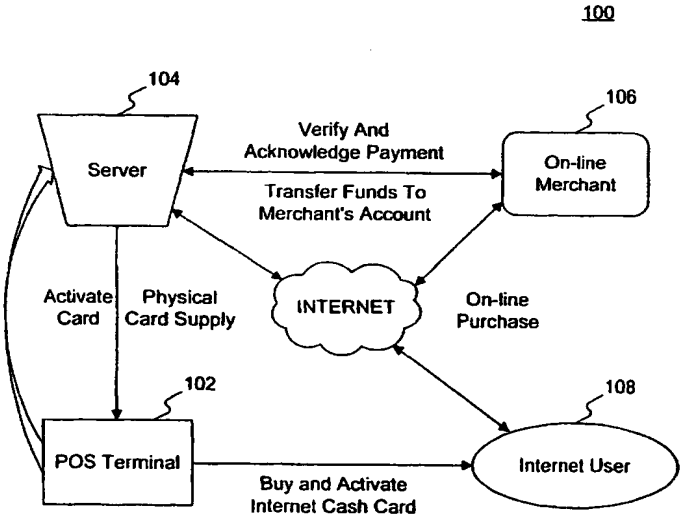
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR MAKING ANONYMOUS ELECTRONIC PAYMENTS ON THE WORLD WIDE WEB



(57) Abstract: Methods and systems consistent with the present invention provide a simple and easy-to-use system to make electronic payments on the Web. Specifically, methods and systems consistent with the present invention provide anonymity, security and accountability. To do so, pre-paid stored value card ("cash card") including a cash card identification number for a predetermined amount of money may be purchased at a point of sale. To ensure security, Personal Security Codes are established for a user at a server. To use the cash cards, a user may visit a Web merchant, select an item to purchase, and enter the cash card identification number and the Personal Security Code to transmit for confirmation to the server. The server subtracts the cost of the item from the predetermined amount on the cash card.

WO 01/11515 A2

METHOD AND SYSTEM FOR MAKING ANONYMOUS ELECTRONIC PAYMENTS ON THE WORLD WIDE WEB

RELATED APPLICATIONS

Provisional U.S. Patent Application No. 60/136,714, entitled "METHOD AND SYSTEM FOR MAKING ANONYMOUS ELECTRONIC PAYMENTS ON THE WORLD WIDE WEB," filed May 28, 1999, is relied upon and is incorporated by reference in its entirety in this application.

TECHNICAL FIELD OF THE INVENTION

This invention generally relates to electronic commerce on the World Wide Web (the "Web") and, more particularly, to methods and systems for making anonymous electronic payments on the Web.

BACKGROUND OF THE INVENTION

The Web has evolved into a new commercial environment with enormous potential. Fueled by its universal appeal, instant and worldwide access, ease of use and low cost of operation, the Web has been the location of choice for a surprising number of merchants, vendors and service providers alike.

To realize the full commercial power of the Web, however, it is necessary to provide efficient payment mechanisms. With a payment-processing infrastructure in place, user (customer) transactions can be completely performed on-line without requiring telephone or other forms of personal communication. This capability is translated to more efficient payment processing, smaller operational costs and, more importantly, a very convenient "click-and-pay" method and system for users to use. All of this further enhances the Web's potential to bring higher revenue to on-line merchants.

The current payment method of choice for the majority of on-line shops is credit cards. Although the use of credit cards is a convenient and commercially accepted method of payment, the use of credit cards presents a variety of problems for users and merchants alike. First, it is necessary for users to obtain a credit-card account. Although this may sound straightforward and more or less a universal practice, a problem is that a large

part of the user population cannot, or will not, have access to a credit card account. Even if the users have credit card accounts, many people still feel uncomfortable using their credit cards on-line. This is because the current level of trust on the Internet is justifiably very low. Credit cards can easily be abused, partly because of very relaxed security measures built into credit cards, and partly because of the longevity of each credit card account. Because of these drawbacks, many users are forced to be extremely cautious when giving their credit card information on-line, which many simply will not even do. Yet another drawback of using credit cards on-line is the extreme accountability of credit cards, that is, someone has to track every user's payment. In addition, there is a lack of personal privacy which further discourages their use over an untrusted and insecure medium such as the Internet. As such, whether it is personal choice, justifiable distrust, young age, limited income sources, or bad credit, the result is that a lot of revenue is lost because potential users cannot or will not use their credit cards on-line.

For merchants too, the current payment process is not an efficient one. For example, merchants have to pass an account setup screening process similar to the one users have to pass; this is mainly because of the relaxed security measures used by credit cards. But in addition to the setup costs, transaction costs and constant fear of being denied their payments due to fraudulent credit card use, merchants have to endure detailed accounting of their credit card payments, process payments in a physical manner, initiate and maintain communication with a clearing house and, in general, put a lot of time and effort into a single transaction. All of this adds up to a very high per-transaction cost.

For these reasons, more convenient and cost-efficient payment methods have been sought in the past. Examples are electronic cash systems (DigiCash, CyberCash), electronic credit card systems (First Virtual, SET), telephone-based Internet payment systems (eCHARGE, iBill), and micropayment systems (Micromint, Millicent). A description of these systems follows: CyberCash

CyberCash makes software for secure financial exchanges via the Internet. CyberCash acts as a gatekeeper linking the Internet to bank networks using security based on cryptographic authentication and encryption. The user sends CyberCash their credit-card number or bank account information, and CyberCash gives them an "electronic wallet" that records their transactions over the Internet, encrypts the payment, and sends it to the merchant. In its instabug model, the user establishes a pre-paid instabug account. Buyers hit the "pay" button on the World Wide Web page to transfer the funds from their accounts to the merchant's CyberCoin cash register.

DigiCash

DigiCash's electronic cash, called eCash, is paperless money that can be transferred on the Internet. A computer user withdraws eCash electronically from a bank that also subscribes to the system. The digital dollars are stored on the user's hard drive and can then be used in a transaction with an on-line merchant who accepts eCash.

eCHARGE

A user chooses a product at a web page where eCHARGE is available, where the freely available eCHARGE software automatically downloads and connects the user's computer to a 1-900 number. Charges for the product later appear on the monthly local telephone bill.

E-cash

E-cash is an instantiation of DigiCash's eCash which is used in conjunction with the Mark Twain Bank to allow "authentication" of digital cash withdrawals from bank accounts. A software program enables storing the withdrawn digital cash on the user's computer hard disk. This stored "cash" can then be transferred to a seller's machine. In this system, participants must set up a World Currency account provided by the Mark Twain Bank.

First Virtual Holdings

To use the First Virtual Holdings system the user opens an account and is given an Identification (ID) number which is sent to the merchant via e-mail. The merchant forwards the e-mail to First Virtual to verify the user's ID

number. First Virtual then sends an e-mail message to the user to verify the transaction. First Virtual performs the actual transfers over a private off-line network using Electronic Data Systems (EDS).

iBill

Similar to eCHARGE, users can bill one-time charges with iBill's Web900 service for access and services directly to their phone bill. The Web900 Instruction Page on the merchant's web page tells users how to dial an appropriate iBill-maintained 900 telephone number to pay for their purchase. When the user dials the 900 number, iBill's automated voice system reads out a series of numbers. The user then returns to the merchant's site and enters these numbers in order to redeem their purchase.

Millicent

Millicent, offered by the Digital Equipment corporation, is electronic "scrip" in the form of a signed message carrying a serial number and an expiration date. An authorized broker will buy Millicent scrip from one or more merchants at a volume discount and then sell it to users, who will receive and then spend it over the Internet.

NetBill

NetBill is an alliance between Carnegie Mellon University and Visa, designed to allow information to be bought and sold over the Internet. Users deposit money into a NetBill account which is drawn upon by NetBill when purchases are made.

Smart Cards / Stored Value Cards

Many prior art schemes involve the use of Smart Cards and Stored Value cards at a user's computer via a personal swipe or chip reading hardware that would read the value of the stored currency on the card's embedded computer chip, and transfer purchasing information on-line to an accepting merchant. The same system can be applied to credit cards and bank-issued debit cards.

SET

Secure Electronic Transactions is a system designed by MasterCard and Visa to allow secure credit card transactions over the Internet. The

system requires credit card clearing houses, merchants and users to download and install the appropriate software. The credit card information is sent encrypted between the user and the merchant and is verified at the clearing house, without exposing it to other users of the Internet or to the merchant himself. Digital signatures authenticate each transaction for future auditing.

The on-line market, therefore, still lacks a simple and easy-to-use "click-and-pay" method and system of making electronic payments which promotes spur-of-the-moment purchases and payment habits and which affords anonymity, security and accountability.

SUMMARY OF THE INVENTION

The invention is directed to a simple and easy-to-use method and system of making electronic payments on the Web that provides anonymity, security and accountability. The computer-based method for making payments on the Web includes the steps of purchasing a pre-paid stored value card ("cash card") including a card identification number for a predetermined amount of money at a point of sale; logging on to a cash-card web server to establish a Personal Security Code (User PIN); logging onto a Web merchant; selecting an item to be purchased; and entering the card identification number and the User PIN, wherein the cost of the item is subtracted from the predetermined amount on the cash card.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an implementation of the invention and, together with the description, serve to explain the advantages and principles of the invention. In the drawings,

Figure 1 is a block diagram of a communication model in accordance with an embodiment of the invention for conducting electronic commerce;

Figure 2 depicts a flow chart of the steps performed when performing a sale at the point-of-sale (POS) in accordance with methods and systems of the present invention;

Figure 3 depicts a flow chart of the steps performed when signing up an on-line merchant in accordance with methods and systems of the present invention;

Figure 4 is a flow chart of an on-line payment process in accordance with methods and systems of the present invention; and

Figure 5 depicts a more detailed diagram of the server depicted in Figure 1.

DETAILED DESCRIPTION OF THE INVENTION

The following detailed description of the invention refers to the accompanying drawings. Although the description includes exemplary implementations, other implementations are possible, and changes may be made to the implementations described without departing from the spirit and scope of the invention. The following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims. Wherever possible, the same reference numbers will be used throughout the drawings and the following description to refer to the same or like parts.

In the following sections, the Web browser, architectural overview of the invention, InternetCash℠ payment cards, point-of-sale terminals for distributing the cash cards and a merchant's system are described. In addition, a step-by-step payment procedure, the InternetCash℠ payment system server architecture and alternate embodiments of methods and systems consistent with the present invention are described.

Overview

The commercial power of the Web has not yet been fully utilized. The biggest hurdle has been the availability of an easy to use "click-and-pay" computer-based electronic payment method and system. This capability is translated to extremely efficient payment processing, smaller operational costs and, more importantly, a very convenient "click-and-pay" computer-based method and system for users to buy goods. All of which further enhance the Web's potential to bring higher revenue to on-line merchants. Methods and systems consistent with the present invention enable users to

buy pre-paid cards at, for example, a convenience store, activate their card by selecting a PIN at a specified server, click on a payment button at their site of choice, and enter their card number.

Merchants may also register at the server to open an account and download the payment software which can be inserted into any web page. The computer-based methods and systems consistent with the present invention offer user anonymity (via the anonymous purchasing channel), accountability, simplicity, speed of use, and the ability to accept micropayments.

The invention provides many advantages over the current systems as described below by combining electronic verification, which is the minimum requirement for on-line payments, with a physical distribution-based pre-paid cash card, which is the most convenient way of distributing value. In particular, the invention makes electronic verification more efficient, and by combining electronic verification with pre-paid cash cards, the invention provides a convenient and efficient method and system of making electronic payments on the Web. The pre-paid cash cards allow payments on the Web without requiring an account to be set up and offer anonymity to the users. Further, no account-opening or software download procedure is required of the users. This allows every user to shop, and promotes "spur-of the-moment" purchasing behavior, which is a significant advantage for on-line shopping.

The World Wide Web

The Web is a globally connected network and operates on a client/server model. A user runs a Web client on a computer called a Web browser such as MOSAIC®, NETSCAPE® or INTERNET EXPLORER®. The Web client contacts a Web site on a server and requests information or resources. The server locates the information and then sends the information to the Web browser, which displays the results.

To use the Web, a user makes an Internet connection and launches a Web browser. When users surf the Web, they view multimedia home pages (Web pages) composed of text, graphics and multimedia content, such as

sound and video in a browser. The user may enter a Universal Resource Locator (URL) in the browser specifying a location (server) to visit. The user may also "click" on a link to forward the user to a new location.

When a server finds the requested home page, document, or object, the server sends the information back to the Web browser.

A Web browser displays information by interpreting the Hypertext Markup Language (HTML) used to build home pages. The coding in the HTML files tells the browser how to display the text, graphics, links and multimedia files on the home page. The HTML file that the browser receives from the server does not have graphics, sound, multimedia files and other resources on it. Instead, the HTML file contains HTML references to those graphics and files. The browser may use the references in the HTML file to find the files on servers, and display it as a home page in the browser.

The Web browser typically runs application programs that are written in JAVA®, a computer language developed by SUN MICROSYSTEMS®. JAVA® is a programming language that allows programmers to create interactive programs and add multimedia features to home pages. JAVA® is object-oriented. Object-oriented programming languages are created by pre-existing components, instead of having to write the entire program from scratch. NETSCAPE is an example of a Web browser capable of running JAVA® programs. JAVA® programs that run at the client inside a browser are called "applets," such as new stickers which run across Web pages, and animations.

When a user visits a Web site or server that contains JAVA® applets, each applet is downloaded to the user's computer from the server. Once the applet is downloaded it runs automatically. These advances have allowed the Internet to become one of the primary places that businesses operate, and where billion of dollars of goods and services will be bought and sold every year. As businesses use the Internet to market and sell their products, many people will buy things while at home and from their place of business instead of at retail stores. They will use the Internet to browse through catalogs and make purchases online.

The nature of the Internet, however, is that it is an insecure network. As packets travel across the Internet, any user could conceivably examine the packets. Because of the Internet's insecure nature, there are potential dangers to doing business online. If a user provides credit card information on the Internet, a third party could steal the credit card number and other identifying information. Software engineers have developed schemes to transmit confidential information securely to combat ths problem. This is known as encryption and decryption.

Information to be sent needs to be encrypted, that is, altered so that to third parties the information will look like meaningless garble. The information also needs to be decrypted, that is, turned back into the original message by the recipient, and only by the recipient. Many complex systems known as "cryptosystems," have been created to allow for this kind of encryption and decryption.

The heart of understanding how cryptosystems work is to understand the concept of "keys." Keys are secret values used by computers in concert with complex mathematical formulas to encrypt and decrypt messages. For example, if a user encrypts a message with a key, only a user with a matching key could decrypt the message. There are two kinds of common encryption systems: secret-key cryptography, also called symmetric cryptography, and public-key cryptography, also called asymmetric cryptography.

In secret-key cryptography, only one key is used to encrypt and decrypt messages. Both the sender and receiver need copies of the same secret key. In contrast, public-key cryptography uses two keys (a public key and a private key). Each user (sender and recipient) has both a public key and a private key. The public key is made freely available, while the private key is kept secret on the user's computer. The public key can encrypt messages but only the private key can decrypt messages that the public key has encrypted. If a sender wants to send a message to a recipient, for example, the sender may encrypt the message with the recipient's public key. But only the recipient, with the private key, could decrypt and read the message. The public key

could not decrypt the message. An example of public/private-key cryptography is the well-known Pretty Good Privacy (PGP) encryption system.

Architectural Overview

Methods and systems consistent with the present invention disclose a communication model, underlying cryptographic algorithms, and system requirements that are simple to use while ensuring security, anonymity and accountability.

An advantage of the invention is that it limits the number of interactions and communications between participants. Figure 1 shows an embodiment of a communication model 100 of the invention, also known as "InternetCash℠."

In model 100, InternetCash℠ payment cards are first transferred to a physical point-of-sale (POS) terminal 102. A POS may be located in any physical store, such as a supermarket, pharmacy, convenient store, or be a dispensing terminal similar to an automated teller machine (ATM). At this point in the preferred embodiment, the cards are inactive which makes the value of the cards negligible and thus minimizes the amount of security needed for transportation and before any sale at POS terminal 102. Thus, the cards can be handled and displayed freely. In fact, products such as camera films, batteries, off-the-shelf medications have a more concentrated value (value per volume) than the cash cards at this point. Because of the low value of the cash cards, the cards can be supplied using the same channels as other physical products and do not have to be kept in a secure location.

Activation Procedure

Before the cards are usable, an activation procedure is performed. In the preferred embodiment the cards are activated at the time of purchase. In the case of a POS at a physical store, activation is performed via on-line communication with an on-line banking system server 104, such as InternetCash℠. The on-line communication may be through pre-existing means, for example, a card reader with dial-up capabilities or manually via the telephone. A store-specific personal identification number (PIN) and a store identifier (SID) may be used for accountability of activated cards. The SID may be used as a store/terminal unique identifier and as a countermeasure

against brute force attacks against the PIN. The SID is kept secret and if possible it is sent to server 104 upon card activation. Otherwise the store PIN is used as an identifier instead.

Similar to the SID, the PIN prevents impersonation of a store clerk and false card activation. The larger the number, the lower the risk of it being decoded. This is not, however, convenient for the store clerks and may lead to typographical errors so the standard credit-card store PIN is used (e.g., 4-8 digits). Measures such as tracking of repeated failed logins using the PIN may be taken to prevent brute force attacks. However, depending on store requirements the PIN may be the same for all clerks or the PIN may be used not for security but simply for indicating the function of card activation.

Cards may also be purchased from an ATM terminal. The ATM-dispensed cards may be activated, for example, by on-line communication (described above), or by off-line activation. An example of the off-line activation may be when a terminal prints out an "activation receipt" corresponding to a specific dispensed card. This receipt contains a portion of the secret number required for card usage. In either case, the terminal should be as secure as a typical ATM terminal because it holds approximately as much cash as an ATM (either dispensed cash like an ATM and/or received cash by the user) and the terminal contains a secret key used either for secure on-line communication or for potential generation of the "activation receipt." In an alternative embodiment, the dispensed cards may be active at time of shipment, so an additional activation is not necessary; such cards should be treated as cash as far as liability is concerned.

In addition to the activation procedure at POS terminal 102 or at an ATM terminal there may be an additional authorization procedure performed by the user. The authorization procedure creates additional security, however, a system without the activation procedure may still be secure if the manufacturing process of the cards is controlled. First, a user logs into server 104 and is asked for the card number and card secret code. Alternatively, a first time user may first need to be authorized by server 104. Server 104 may ask the user for the card number and card secret code again. Server 104

subsequently accesses the record of the entered card number, verifies the card secret code, and that the card has not previously been authorized. Server 104 them asks the user to enter a User Personal Security Code (UPIN). The UPIN may be between 4 and 8 characters. The UPIN and associated card number may be stored in a database at server 104, such as an ORACLE® database. The activation procedure also affords added security to the user, by not allowing a lost card to be spent if the UPIN is not available.

The "click-and-pay" methodology using an InternetCash℠ payment card will now be explained. First, a user 108 logs in to a web site associated with merchant 106 and upon selecting a product/service, clicks, for example, a "click-and-pay" button. If user 108 is a first-time user, user 108 may be transferred to server 104 to automatically download any required software. If the user is not a first-time user, or once the software is downloaded, a window at the user's computer requesting the InternetCash℠ payment card number may be displayed. Payment information may also be displayed in the window for user verification. A merchant number and transaction-specific number may be stored at the user's computer for future accountability.

After entering the InternetCash℠ payment card number in the display window, a payment-specific authentication number (PAN) is sent to server 104 (or the merchant forwards it) along with the payment data and the card number. The PAN is an authentication of the payment information that functions as a Message Authentication Code (MAC). To prevent collision attacks, current MACs must be 160 bits and can be based on a hash function, such as the well-known SHA-1 functions. This size should afford sufficient protection while 256 bits are projected to provide adequate security for the next 25 years. Once received, server 104 may process the transaction. Server 104 verifies that the card is active, the PAN has been computed correctly, the requested amount is available on the card, subtracts the payment amount from the card and credits the amount to the merchant's account, and returns an acknowledgment to merchant 106 as well as user 108. Alternatively, merchant 106 may forward the acknowledgment from

server 104 to user 108. This information may also be stored at user 108's computer. If the transaction succeeds, then merchant 106 may provide the product/service to user 108 using any well-known delivery service, such as UPS, or by electronic delivery, such as HTTP, or FTP.

If merchant 106 fails to deliver the product/service once the card has been debited, then user 108 may contact server 104 and provide the payment data and the transaction-specific number (PAN) previously received during the processing of the transaction. Server 104 may determine if user 108's card has been charged for this transaction. If the user 108's card has not been charged, the transaction data is deleted from the database. If the user 108's card has been charged, then either merchant 106 did not provided the requested product/service, or user 108 has not received them or acknowledged their receipt. In either case, this is an exception condition, which may be handled according to a merchant/InternetCash℠ policy. Server 104 may also log such events. The click-and-pay methodology is further described below with reference to Figure 4.

Account Cards

The cards which are used for InternetCash℠ for payment on the Web will now be described. The first kind of cards which may be used are magnetic-stripe cards that are dispensable by store clerks. On their backside, the cards include: a card ID, a card secret code and directions for using the card and potentially a server's telephone number. If present, server 104's telephone number may be used for dialing in for on-line verification; otherwise on-line verification is performed via the magnetic stripe, as explained below.

Each card has its own Card ID (CID). The CID is a character alphanumeric code comprised of 10 numeric digits and 26 letters. The size of the CID is determined as follows: assuming a user base of 1 billion users, each user uses two cards a day for a period of 25 years (that is, before the CID size needs to be changed), and there are two types of dispensing systems. This amounts to about 45 bits, or 8.7 (9-10) alphanumeric characters. This is based on the calculation that one alphanumeric character has 36 different combinations (0-9 and A-Z) thus corresponds to $\log_2 36 \approx 5.17$

binary digits (bits). Therefore 45 bits correspond to 45 ÷ 5.17 ≈ 8.7 alphanumeric characters. For example, for a CID = 6, there are approximately two billion possible CIDs since each alphanumeric character represents 10+26 = 36 different combinations. With $36 \approx 2^{5.17}$, each alphanumeric character is equivalent to 5.17 bits. Thus 6 alphanumeric characters are equivalent to 6*5.17 = 31.02 bits; and there are $2^{31.02} \approx$ 2,177,461,402 or approximately 2 billion combinations.

This CID number does not need to be kept secret and may be visibly displayed on the card. The Card Secret Code (CSC), however, must be kept secret. The CSC is used to provide security for the card. The CSC is a character alphanumeric code comprised of the same alphabet of numbers and letters as the CID, but it is not displayed on the card, so that only the user has this information. The CSC is further described below.

The directions for using the card include instructions to verify that the card was indeed activated (an activation receipt may be printed out at POS terminal 102) and that the client software at the user 108's computer being used at payment time (the payment window) is authorized. The software is verified either by downloading it securely from server 104, verifying that code (e.g., applets) downloaded from a merchant is digitally signed by server 104, or verifying that the payment window is served from server 104.

The magnetic-stripe may also contain a Bank Identification Number (BIN), the card ID, and server 104's telephone number. There are two types of cards that may be used, the type with a scratch-panel and the type without a scratch-panel. The scratch-panel type cards use the scratch panels to hide the CSC. Once a user buys the card the user may scratch off the scratch panel to reveal the CSC. Since the card contains hidden information, only user 108 knows the number. A warning may be displayed on each card to prevent user 108 from buying the card if the panel has been scratched off.

The cards without scratch-panels are similar to the cards with scratch panels in that the CSC is typed on the card and covered. The cards without scratch-panels may be glued to a paper holder and, thus, the CSC may only be seen after user 108 has removed the card from its holder. Alternatively the

holder completely encloses the card, so that again the card secret code is not exposed unless the cover is ripped opened. A warning may be displayed on such cards such that they should not be purchased if the holder has been removed.

An alternative to the magnetic-stripe cards is a simple flexible plastic card containing the same information as the magnetic-stripe card. With the plastic cards, however, a store clerk first dials up server 104 and enters the CID to perform on-line activation. Alternatively, these cards are activated at shipping time and do not need to be activated at the time of sale. Similarly to the magnetic-stripe cards, there are two types of plastic cards: the type with scratch-panel for protecting the secret code and the type without scratch-panel.

Cards may also be dispensed from an unmanned ATM-style terminal. These dispensed cards do not need a magnetic-stripe or a scratch-panel because there is no human involvement and, as such, there is no danger of stealing the CSC code. Instead, the CSC is calculated and given to the user by the terminal. This calculation is performed using a terminal-specific secret key (TSK) and a cryptographic one-way or hash function. The TSK is further described below.

The CSC is either printed on the card at the time of sale, on a separate "receipt" paper, or is simply shown to user 108 who is prompted to write the code on the card. The dispensed cards may be made of materials, such as paper, plastic, or a magnetic-stripes. The paper cards may be printed on the fly by the terminal since most ATM machines have a printer. This requires no dispensing system. The paper cards contain the CID and directions for usage. The ATM may print the card and include the CSC on the card.

The flexible plastic card may or may not require some type of low-security dispensing mechanism, but provides a "tangible" material for user 108. Finally, the magnetic-stripe cards allow reloading at any POS 102. The magnetic-stripe cards, however, are more expensive and may require a method of securely dispensing to prevent theft. Additionally, the magnetic-

stripe cards may contain server 104's telephone number and/or the BIN and CID numbers.

In an alternative embodiment, pre-activated cards may be dispensed from separate canisters within an ATM machine. ATM machines have separate canisters that hold products, such as stamps, or checks. These ATMs also include software that prompts user 108 and subtracts funds from a user 108's account when user 108 purchases items from the canister. Cash cards may be dispensed from ATM machines using these canisters.

POS Sale

Figure 2 depicts a flow chart of the steps performed when performing a sale at the POS Terminal 102 consistent with methods and systems of the present invention. As discussed above, there are two forms of sales. Sales at a store using a POS terminal 102 (manned sale) and sales at an ATM terminal (unmanned sale). With a manned sale, the store clerk's role is to activate the card.

First, a secure connection to server 104 is established (step 202). Typically, this is a dial-up session but an Internet connection is also possible depending on the facilities available at the POS Terminal 102. If a magnetic card is used, then the dial-up connection may be performed by using an existing card-reader with dial-up capabilities used for credit-card authentication. In this case the BIN number and/or the telephone number of server 104 is encoded on the magnetic-stripe so all that is required from the clerk is to simply slide the card through the reader and select the appropriate button for card activation.

Once connected, the store clerk may input a CID and a store-specific PIN that are then transmitted to server 104 (step 204). The CID may be encoded on the magnetic-stripe so this is sent automatically to server 104. The clerk may then input a store-specific PIN to activate the card.

Alternatively, the cash cards may be activated in batch form, (e.g., five or ten) such that each card need not be activated as it is sold. In a batch mode, the clerk inputs the batch number of the cards, which identifies that

particular batch. If the dial-up device supports encryption and authentication, the batch mode may be utilized over this link.

Next, server 104 may process the transaction (step 206). During processing, server 104 activates the particular CID or card. The store's PIN may be saved together with the activation record (CID or batch and timestamp). Merchant 106 may be charged immediately or periodically, such as once a day. In addition, an acknowledgment may also be returned as part of processing the transaction and a receipt may also be printed for user 108.

Alternatively, the POS method may be performed by an unmanned sale. Depending on the payment scenario, either a secret key inside POS terminal 102 needs to be secured or the POS terminal 102 may have a secure dispensing canister (in the case where the card is paid by withdrawing cash directly from a user 108's bank account). In the case where user 108 pays by cash terminal 102 should also accept cash. For example, ATM machines require both a secured secret key and the ability to store cash and also include secure dispensing canisters.

There are several scenarios for the unmanned sale, depending on both the POS terminal 102 and type of card used. For example, in an ATM-bundled sale, a bank ATM may provide user 108 an additional choice of "Buying an InternetCash℠ payment card." If user 108 desires to purchase an InternetCash℠ payment card, user 108 may select desired values, such as ten dollars or one hundred dollars. The ATM withdraws an appropriate amount from user 108's bank account and prints the card including the CID, CSC, directions for use and a transaction receipt. Alternatively, a set of blank cards may be located next to an ATM and user 108 may be required to write (with an attached pen) the CID and secret code on each card. This provides for a more "tangible" card. The ATM may then notify server 104 that a specific card has been sold. Alternatively, the ATM may notify server 104 at a later time, such as once every night for all cards sold that day. The ATM may then further process a list of available CIDs and a secret key which can be used to compute the card's secret code. The CIDs are unique in that they do not require explicit activation, and are activated in advance. Security

may also be provided by a controlled generation of the secret codes, based on the ATM's secret key. The ATM secret key (TSK) is specific to each ATM used to compute the CSC. The secret key is inserted securely (for example, by designated personnel, or via a secure channel) and is generated by server 104 based on a master key and a unique identifier, such as the exact location and bank name of a particular ATM. In an alternative embodiment, pre-activated cash cards are provided in a secure dispensing canister, and after collecting money from user 108 may dispense the cards similar to how cash is dispensed. In this case, cash cards are formatted to a size similar to a paper bill and include a scratch panel similar to the cash cards sold by a store clerk.

In an alternative embodiment, a cash-terminal sale accepts cash. Instead of accessing a user 108's bank account as in the ATM terminals, the cash-accepting terminals accept cash. A cash-accepting machine only needs a printer and does not need a display.

Additionally, a cash accepting machine may be used to dispense pre-activated cards stored in a secure canister. This machine does not need specific additions, with the only requirement being secure transfer of cash cards and positioning them into the canister.

CID Generators

Examples of CID generators, secret and master keys, and terminal identifiers will now be described.

(1) CID: In the case of point-code tracking the CID may be a concatenation of binary digit "1" (denoting point-code tracking) and a terminal unique identifier (TID) (8 decimal digits) to an ever-increasing serial number. Point-code tracking is defined as allowing tracing in dispensing terminals using the CID and by generating secret code on-the-fly by unmanned terminals.

In the example where the CID is the concatenation of the TID and a serial number, the CID discloses the TID and thus the dispensing terminal. The TID number is based on an assumption that there are 100 million terminals. These numbers are converted to binary, concatenated and converted to alphanumeric characters (base 36).

Thus, assuming there are 100 million dispensing points with each dispensing point dispensing a maximum of 2,500 cards per POS per day for two types of dispensing systems (point-code tracking and user-based) over a 25 years system life, this amounts to 51 bits, or 10 alphanumeric characters. Thus the number of cards over 25 years = 100,000,000 (dispensing points) * 2,500 (cards per day per dispensing points) * 365 (days in a year) * 25 (years) ≈ 2,281,250,000,000,000 ≈ 2^{51}. Thus the number of cards over the next 25 years can be represented with 51 bits, which amount to 51 ÷ 5.17 ≈ 9.86 alphanumeric characters.

Cards and CIDs may be generated inside a cash card terminal by using a pseudorandom or sequential algorithm. The same space on the cards should not used for both point-code tracking and regular cards. For example, the regular CIDs may start with a binary digit "0." The batch cards may also contain a batch number which can optionally be printed on the cards. The batch cards may be packed in batches and/or be activated in batches, either through a web interface within server 104 or through a phone interface.

(2) Internet Master Key (IMK): The IMK is created in a cryptographically secure way, and may contain over 160 bits. The IMK may contain random bits that are processed by a cryptographic function, such as a one-way hash function. These random bits may be created as a combination of inputs, including the InternetCash℠ administrator's keystroke, mouse movements, hard-drive speed variations, operating system state, time variations between hardware clocks, or other hardware sources of randomness, such as oscillators, or lava lamps.

A brute force attack against the IMK could allow total manufacturing of cards. In this context, a "brute force attack" is the case where the attacker tries all possible values of a secret key, in this case the IMK, until the correct value is found; thus, at least 128 bits must be used, and preferably 256 bits. The IMK may expire at any time and cards manufactured after that point should use a new key. It is preferable that the IMK be refreshed at regular intervals (for example, annually) and be stored in a tamper-resistant hardware cryptographic device.

(3) Terminal Secret Key (TSK). CSC = H(TSK, CID), where H is a cryptographic hash function. TSK may in turn be calculated using an IMK and the TID in combination with a cryptographic one-way or hash function; for example TSK = H(INK, TID), where H is a cryptographic hash function. This is generated by the IMK as follows: TSK=H(IMK, TID), where H is a one-way hash function or a block cipher (in which case IMK is the key) whose output is casted (truncated) to the required size for TSK.

Brute force attacks against the TSK key could allow manufacturing of cards for a particular terminal. Since the terminal can be "black marked," this type of attack may not be very costly. In other words, if the terminal's key is lost, the terminal identifier can be marked as invalid starting from the time of security breach and ending at the time where the terminal is repaired, and all cards that are manufactured by this terminal in this time interval are also deemed as invalid. It is preferable that an 80-128 bit key be used, but if convenience dictates, a standard 56-bit DES key may be used.

(4) Card Secret Code (CSC). The CSC key is used to generate the Payment Authentication Number (PAM). For a CSC = 10, the card is secured with a secret key of approximately 10*5.17 ≈ 51 bits. Brute force attacks require either querying the server 104 for each attempt or verifying against a payment, which is much more efficient. However, only one card is impersonated if such an attempt succeeds, so we need to solve for:

Cost of brute force > value of card.

The CSC is generated using the TSK as follows:

CSC=H(TSK, card ID),

where H is either a one-way hash function or a block cipher (in which case TSK is the used key) casted (truncated) to the required size for CSC (11-16 alphanumeric digits). In sum, server 104 may generate the CSC given the CID and IMK. That is, from the CID, server 104 obtains the terminal identifier TID and computes TSK (TSK = H(IMK, TID)) and, finally, the CSC (CSC = H(TSK,CID)). Server 104 may now verify that the card has been generated ("activated") by a designated terminal.

For non-point-code tracking cards, the CSC can be calculated directly from the IMK and the CID:

CSC = H(IMK,CID).

It is expected that 56 bits are enough for small card values (<$100) for a 5-year period (a goal is to prevent users from cracking cards at their desktops). Eighty bits are enough even for large card values. It should be reminded that brute force attacks require theft of payment, which is transmitted over SSL; "SSL" refers to the Secure Sockets Layer protocol which is being utilized for encrypting and authenticating data that is sent over the Internet or other insecure or public lines; SSL is a de-facto standard used by Netscape Communicator ®, Internet Explorer ®, and other commercial browsers.

(5) A PAN used for authentication may be calculated as follows:

PAN=H(CSC, UPIN, Payment Info),

where H is a hash function (or a block cipher, in which case CSC and UPIN are used as key.

On Line Registration

Figure 3 depicts a flow chart of the steps performed when signing up an on-line merchant 106 and user 108. First, on-line merchant 106 obtains a registration number and an account at server 104 (step 302). To register, on-line merchant 106 may log onto a web site and fill out an on-line application. Alternatively, on-line merchant 106 may communicate with an InternetCash℠ account representative. Depending upon the type of reimbursement on-line merchant 106 chooses, the application is approved either automatically or after appropriate background credit checks. Once the account is opened and authorized, a merchant identification number is assigned to merchant 106 which may be different from the account number for security purposes.

Next, server 104 sends (or the merchant may download) a signed, "payment program" to merchant 106 (step 304). This program may be, for example, a JAVA® applet that can then be incorporated inside any web page associated with merchant 104, or a program that includes sample web pages and other processing code that interfaces with merchant 104 associated with

a back-end system. The code may be signed by server 104 and based on a public key. The public key is certified by a Certification Authority (CA), such as VERISIGN. The code comes complete with everything that is needed to process a payment, such as plug-ins for merchant 106 to add payment information and code for displaying the payment information. The plug-ins are for information such as dollar amount of purchase, description of product(s) sold, date and time of product sold and an empty "comments" section for additional information (this acts as a "memo" on a personal check). Any code sent to user 108's computer during a purchase, includes programs for displaying the payment information, including merchant 106's identifying information, programs for user 108 to enter additional comments, programs asking user 108 to enter their InternetCash℠ payment card number and UPIN, and programs allowing the signing (or authenticating) of the payment information using the card's secret code and UPIN as the key.

The payment window code is used to send the payment information and a PAN to server 104 potentially through redirection to the merchant, and waits for confirmation from server 104, including the categorized payment information. Server 104 processes the transaction received from payment window code at merchant 106 and sends a confirmation of payment to the payment code window, either directly or through merchant 106.

Additionally or alternatively, the payment program may be personalized for each merchant 106. Merchant 106's identifying information may be displayed in the program as a headline, ticker, or border of the payment window, and may be included in the InternetCash℠ generated signature. This way, only authorized merchants 106 can use the payment program, and provides for greater accountability within model 100.

The instantiation of the merchant-specific program signing can be performed by the addition of the merchant identifying information into the payment program, before server 104 signs the confirmation. In addition, the merchant-specific program signing enables server 104 to outsource the signature authorization and certification to an external CA.

On Line Purchase Method

Figure 4 depicts the steps performed when a user 108 uses the on-line payment process. First, user 108 logs into a Web site associated with merchant 106 and selects the goods/services to be purchased (step 402). If user 108 is a first-time user, user 108 may be forwarded to server 104 for an automated downloading process of the required software (e.g., payment window code). If user 108 is not a first-time user, or once the software is downloaded, a window at user 108's computer requesting an InternetCash℠ payment card number is displayed (step 404). In response to user 108's selection of goods to purchase, the merchant payment program provides the product information, the merchant's identification number, a payment serial number, the payment amount and, optionally, a transaction time stamp to the payment code window on user 108's computer (step 406). The information is displayed to user 108 either through the code (e.g., JAVA® applet), as a redirection from server 104, or through a client resident program (e.g., a browser plug-in). Once the merchant software transmits the information to user 108, the merchant payment program waits for a payment acknowledgment from server 104.

After the optional verification of the InternetCash℠ signature by the payment code window, user 108 verifies the payment information, optionally adds any comments in the comment area and enters the InternetCash℠ payment card number and UPIN (step 408). Either the payment code window or server 104 may compute the PAN based on the CSC and UPIN. Additionally, the computed information may be locally saved at user 108's computer file indexed by the merchant's identification number and transaction number. Once computed, the payment information and PAN are then sent to server 104 (step 410). Alternatively, user 108 may transmit the information to merchant 106, who may forward the payment information to server 104 (step 410).

Next server 104 confirms the transaction (step 412). During confirmation, server 104 may access the card repository file indexed by CID, verify the card validity, obtain or recompute the CSC and UPIN, verify fund availability, subtract funds from the card account, and credit merchant 106's

account. If the payment information is not correct, user 108 may be given the option to re-enter the data. If the card has not been authorized on-line, (e.g., a UPIN has not already been selected), then user 108 may be redirected to an on-line activation page located at server 104, to select a UPIN, before the payment transaction proceeds. Finally, if the funds remaining on the card are not sufficient to cover the cost of goods to be sold, user 108 may be given the option of using an additional card for the remaining amount.

Upon successful completion of step 412, server 104 returns an acknowledgment to merchant 106 and user 108, indexed by a merchant number and a transaction number and a transaction time stamp (step 414). The signature may be based on an IMK. The merchant payment software and the payment code window saves this information in a local file. However, only the merchant software needs to verify the signature's validity before sending the product(s) to user 108 (step 416).

The verification of the InternetCash℠ payment card signature on the payment information and PAN at merchant 106 computer are performed automatically by the payment software. This returns an "accept" code to the merchant, who then may initiate the shipment process.

Disputes over payments and deliveries may be handled based on all saved information merchant 106 and user 108. If, for example, merchant 106 did not send the paid-for products, then user 108 may provide the payment information and acknowledgment to server 104 to verify their validity.

System Design

Figure 5 depicts a system 500 running on a reliable and secure platform. Server 104 may be, for example, an NT® or Unix®-based server on a SUN® workstation. All cryptographic operations are performed inside server 104. Server 104 is connected to a database 502 that contains a list of all issued cards, separated as active and inactive, and all transactions performed by each card. Database 502 may be an encrypted and signed 24x7 database. Cards in server 104 may be indexed by the CID. Each card entry contains the manufacturing date and time, the date, time and location of activation, the total value and the remaining value. A modem pool 504 may

also be connected to server 104 to accept dial-up connections from POS's. Front end web server 506 contains a firewall and an HTTP front end 508 to provide security to server 104. The web server 506 serves as an intermediary between server 104 and network 510.

Conclusion

The invention as described above is a novel solution which can be used by any user without requiring specific knowledge or even software installation. Methods and systems consistent with the present invention require no user accounts, provide anonymity and simplicity of use, and are nevertheless secure and accountable as any cash system should be.

As explained, methods and systems consistent with the present invention overcome the shortcomings of existing financial transactional systems by providing users the ability to spend on-line easily, safely, anonymously, in small or large increments with no personal attachment to Internet service providers, billing, credit card, or banking institutions.

The foregoing description of an implementation of the invention has been presented for purposes of illustration and description. It is not exhaustive and does not limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the invention. For example, the described implementation includes software but the present invention may be implemented as a combination of hardware and software or in hardware alone. The invention may be implemented with both object-oriented and non-object-oriented programming systems.

Attached is an appendix of exemplary number sizes for the various keys.

Appendix

The quantities defined here are cryptographic key sizes within the system of the invention, as well as some assumptions regarding the size of the user base and POS terminals.

Quantity	Size
CID (Card ID)	9-10 alphanumeric chars
CSC (card Secret Code)	11-16 alphanumeric chars
1 alphanumeric character (0-9, A-Z)	=5.17 bits = 1.55 decimal
1 alphanumeric character (0-9, A-Z, except I,O,Q,Z)	=5 bits = 1.5 decimal
SID (Store/terminal ID)	20 decimal digits
PIN (Store/clerk PIN)	6-8 decimal digits
1 decimal digit	= 3.3 bits
TID (Terminal ID)	8 decimal digits
IMK (InternetCash℠ symmetric Master Key)	128-256 bits
TSK (ATM/Cash Terminal symmetric Secret Key)	56-128 bits
PAN (Payment Authentication Number)	160-256 bits
IPK (InternetCash℠ public key)	1024-4096 bits
UPIN (User PIN)	4-8 alphanumeric digits

WE CLAIM:

1. A computer-based method for making anonymous payments in a network, comprising the steps of:

purchasing a cash card including a card identification number for a predetermined amount of money at a point of sale terminal;

logging on a Web site associated with a merchant from a user's computer;

selecting an item to be purchased; and

entering the cash card identification number,

wherein the cost of the item is subtracted from an account associated with the cash card.

2. The computer-based method for making payments in a network of claim 1, wherein the step of entering the cash card identification number further comprises the step of entering a personal security code in a server, wherein the server maintains a record of the personal security code.

3. The computer-based method for making payments in a network of claim 2, further comprising the step of verifying that the personal security code is associated with the cash card.

4. The computer-based method for making payments in a network of claim 3, further comprising the step of entering the cash card identification number and the personal security code to obtain the balance remaining in an account associated with the cash card.

5. The computer-based method for making payments in a network of claim 3, further comprising the step of entering the cash card identification number and the personal security code to obtain a list of the transactions performed in an account associated with the cash card.

6. The computer-based method for making payments in a network of claim 1, further comprising the step of entering multiple the cash card identification numbers and personal security codes for performing a single purchase.

7. The computer-based method for making payments in a network of claim 6, further comprising the step of displaying an amount of a purchase

remaining after each cash card identification number and personal security code is entered and an amount available in an account associated with the cash card.

8. The computer-based method for making payments in a network as in claim 1, wherein the step of purchasing a cash card further comprises the step of activating the cash card by transmitting a store-specific personal identification number to a cash card server.

9. The computer-based method for making payments in a network as in claim 1, wherein the step of purchasing a cash card further comprises the step of activating the cash card by transmitting a fixed personal identification number to a cash card server to signal that the cash card is to be activated.

10. The computer-based method for making payments in a network as in claim 1, wherein activating the cash card further comprises the step of transmitting a predetermined amount of money to a cash card server.

11. The computer-based method for making payments in a network as in claim 1, wherein the step of purchasing a cash card further comprises the steps of:

activating the cash card by performing off-line activation; and

printing out an activation receipt corresponding to the cash card and including a secret number.

12. The computer-based method for making payments in a network as in claim 1, wherein the cost of the item plus an additional transaction fee is subtracted from an account associated with the cash card.

13. The computer-based method for making payments in a network as in claim 1, further comprising the step of storing payment information on a user's computer, wherein the payment information includes a merchant number and a transaction number.

14. The computer-based method for making payments in a network as in claim 1, further comprising the step of entering a payment-specific authentication number.

15. The computer-based method for making payments in a network as in claim 1, further comprising the steps of:

storing on a user's computer the cash card identification number; and

receiving a selection for the cash card identification number from a list of saved cash card identification numbers.

16. The computer-based method for making payments in a network as in claim 1, further comprising the step of verifying that the cash card is active and that the requested purchasing amount is available.

17. The computer-based method for making payments in a network as in claim 1, further comprising the step of crediting an amount associated with a purchase to an account associated with the merchant.

18. The computer-based method for making payments in a network as in claim 1, further comprising the step of crediting a purchasing amount minus a fee to an account associated with the merchant, wherein the fee is based on the purchase amount or a fixed fee.

19. The computer-based method for making payments in a network as in claim 1, further comprising the step of sending a purchasing acknowledgment to the merchant and the user.

20. The computer-based method for making payments in a network as in claim 1, wherein the cash card contains a magnetic-stripe.

21. The computer-based method for making payments in a network as in claim 20, wherein the magnetic-stripe comprises a telephone number of a cash card server, a character alphanumeric code card identification, a character alphanumeric code card secret code and directions for using the cash card.

22. The computer-based method for making payments in a network as in claim 20, wherein the magnetic-stripe comprises an encoded cash card number, wherein the cash card number includes a cash card identification number, a bank identification number (BIN), a Lin mod-10 authentication digit and an expiration date, such that the BIN is used to route the magnetic stripe information to a central server for on-line verification.

23. The computer-based method for making payments in a network as in claim 20, wherein the magnetic stripe contains a telephone number associated with a cash card server for on-line verification, a card batch number and directions for using the cash card.

24. The computer-based method for making payments in a network as in claim 1, wherein the cash card is of the scratch-panel type or glued to a paper holder, or a flexible plastic cash card.

25. The computer-based method for making payments in a network as in claim 24, wherein the cash card secret code is hidden in a scratch-panel and is revealed by scratching off the scratch-panel.

26. The computer-based method for making payments in a network as in claim 24, wherein the cash card secret code is covered by the paper holder and is revealed by removing the cash card from the paper holder.

27. The computer-based method for making payments in a network as in claim 1, wherein the cash card is dispensed from an automated teller machine (ATM).

28. The computer-based method for making payments in a network as in claim 27, wherein the ATM contains a Terminal Secret Code to compute a cash card secret code from a card alphanumeric code printed on the cash card.

29. The computer-based method for making payments in a network as in claim 28, further comprising the steps of:

computing the Terminal Secret Code by a cash card server using a master key; and

transmitting the Terminal Secret Code using a secure channel to the ATM.

30. The computer-based method for making payments in a network as in claim 29, wherein the Terminal Secret Code is stored in tamper-resistant hardware within the ATM.

31. The computer-based method for making payments in a network as in claim 30, further comprising the step of providing the cash card secret code to the user.

32. The computer-based method for making payments in a network as in claim 29, wherein the cash card is a paper cash card.

33. A computer-based method for activating a cash card for making payments in a network using a POS terminal, the cash card includes a card identification number and the terminal is assigned an identification number, the computer-based method comprising the steps of:

establishing a secure connection to a cash card server;

inputting the cash card identification number and a terminal identification number; and

activating the cash card identification number.

34. The computer-based method for activating a cash card of claim 33, further comprising the step of storing the identification numbers with an activation record.

35. The computer-based method for activating a cash card of claim 34, wherein the activation record includes the cash card identification number and a timestamp.

36. The computer-based method for activating a cash card of claim 34, further comprising the step of encrypting the identification numbers with the activation record.

37. The computer-based method for activating a cash card of claim 34, further comprising the step of transmitting an acknowledgment notification to the user once the cash card has been activated.

38. The computer-based method for activating a cash card of claim 33, wherein the connection is an Internet connection.

39. A computer-based method for purchasing a cash card for making payments in a network from an automated teller machine (ATM), the cash card includes a cash card identification number, a secret code and directions for use, the computer-based method comprising the steps of:

providing an ATM user a choice of buying the cash card from the ATM machine;

selecting a value of the cash card to be purchased;

withdrawing an appropriate amount of money from an account associated with the ATM user;

printing the cash card, including the cash card identification number, the secret code, the directions for use and a transaction receipt; and

notifying a cash card server that a cash card has been sold.

40. The computer-based method for purchasing a cash card for making purchases of claim 39, wherein the cash card server is notified at a later time for the purchase.

41. The computer-based method for purchasing a cash card for making purchases of claim 39, wherein the ATM cash card is pre-printed and stored inside the ATM.

42. A computer-based method of opening and registering an on-line vendor account with a cash card server having a web site, comprising the steps of:

logging onto the cash card server's web site;

receiving an application from the vendor to accept cash card payments;

approving the application;

opening an account for the vendor if the application if approved; and

assigning a vendor identification number for the vendor.

43. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 42, further comprising the step of approving the application after appropriate background checks.

44. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 42, further comprising the steps of:

entering a user's cash card number and a personal security code;

adding any comment to payment information; and

computing a payment authentication number specific to the payment information and user supplied data.

45. The computer-based method of on-line payment of claim 44, further comprising the steps of:

sending the user's signature, the payment information and the cash card number to a cash card server;

verifying the payment information from the user;

verifying a payment acknowledgment from the cash card server on a payment applet; and

notifying the user of the finality of the purchase.

46. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 42, wherein the approving step further comprises the step of automatically approving the application.

47. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 42, further comprising the step of sending a secret key to the vendor once the application is approved.

48. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 42, wherein the secret key is generated by the cash card server from a master key.

49. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 42, further comprising the step of supplying a signed payment program to the vendor for accepting on-line payments.

50. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 49, wherein the payment program includes identification information associated with the vendor.

51. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 49, wherein the signed payment program is a Java applet.

52. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 49, wherein the signed payment program is a program specific to a back-end system associated with the vendor.

53. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 49, wherein the signature

on the signed payment program is calculated using a cash card server's public key.

54. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 49, further comprising the step of transmitting an applet to the user from the cash card server, wherein the applet enabled the user to authenticate the payment information.

55. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 54, wherein the plug-in areas include an area for a dollar amount of purchase, an area for description of a product sold, an area for the date and time of product sold and an area for comments for additional information.

56. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 55, further comprising the step of authenticating the payment information with the secret code associated with the cash card.

57. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 54, further comprising the steps of:

displaying the payment information in a display window, including the vendor's identifying information;

providing an area inside the applet for the user to enter additional comments;

requesting the user to enter the cash card number inside the applet;

authenticating the payment information using a payment authentication number and the applet; and

sending the payment information and payment authentication number to the cash card server.

58. The computer-based method of opening and an on-line vendor account with a cash card server of claim 42, wherein after the user is registering to the server, the computer-based method further comprises the steps of:

displaying the payment information, including the vendor's identifying information;

providing an area in the page displayed by the PAN server for the user to enter additional comments;

requesting the user to enter the cash card number in an area inside the page displayed by the PAN server;

having the PAN server authenticate the payment information using a payment authentication number; and

sending the payment information and payment authentication number to the cash card server.

59. The computer-based method of opening and registering an on-line vendor account with a cash card server of claim 58, further comprising the step of sending a confirmation of a payment to the user.

60. A computer-based method of on-line payment, comprising the steps of:

logging onto a vendor's Web site, wherein the Web site includes a payment software for providing product information, a vendor identification number, a payment serial number, a payment amount and a transaction time stamp to the payment software;

selecting goods/services for a user to purchase;

displaying purchasing information by the user; and

receiving a payment acknowledgment from a cash card server.

61. The computer-based method of on-line payment of claim 60, further comprising the step of redirecting the user to a PAN server to display purchasing information.

62. The computer-based method of on-line payment of claim 60, further comprising the step of transmitting an applet to the user to display purchasing information.

63. The computer-based method of on-line payment of claim 62, further comprising the steps of:

verifying payment information from the user;

adding comments to the payment information; and

entering a cash card number to finalize the payment of the purchase.

64. The computer-based method of on-line payment of claim 63, further comprising the steps of:

computing a payment authentication number based on a cash card secret code by the applet; and

saving the purchasing information and the payment information locally into a file indexed by the vendor identification number and a transaction number.

65. The computer-based method of on-line payment of claim 61, further comprising the step of sending the payment information and the PAN by an applet to the cash card server.

66. The computer-based method of on-line payment of claim 65, further comprising the step of waiting for confirmation by the applet.

67. The computer-based method of on-line payment of claim 66, further comprising the following steps performed by the cash card server:

accessing a cash card repository file indexed by cash card ID;

obtaining the cash card secret code;

verifying fund availability;

subtracting funds from a user's account; and

crediting a vendor's account.

68. The computer-based method of on-line payment of claim 67, further comprising the following steps being performed by the cash card server:

returning a signed payment acknowledgment to the vendor and the user, indexed by the vendor identification number and the transaction number; and

saving information in a file at both the user-residing applet and the vendor payment software.

69. The computer-based method of on-line payment of claim 68, further comprising the steps of:

verifying the signature's validity on the signed payment acknowledgment by the vendor payment software; and

sending the purchased goods/services to the user.

70. A method for providing a cash card for a user to make purchases in a network anonymously, wherein the cash card is associated with an account containing a predetermined amount of money, comprising the steps, executed in a data processing system, of:

activating the cash card at a point of sale;

authorizing the cash card such that an account associated with the cash card contains funds to make purchases with; and

providing the cash card to a user, wherein a cash card secret code and a cash card identification we associated with the cash card.

71. The method of claim 70, wherein activating the cash card further comprises the steps of:

transmitting a cash card identification number and a point of sale identification number to the server using a secure channel; and

initiating the secure channel with a secret key, wherein the secret key is unique for each point of sale terminal.

72. The method of claim 71, further comprising the steps of:

generating a cash card secret code for each cash card based on a master key; and

generating a point of sale secret code for each point of sale terminal based on the master key,

wherein the cash card secret code is used to authorize the cash card.

73. A method for purchasing products from a merchant over a network using a cash card, comprising the steps, executed in a data processing system, of:

transmitting purchase information to a payment code window associated with the user, wherein the purchase information includes a merchant identification number;

receiving a transaction from a user in a server, wherein the transaction is based on the received purchase information and includes a payment specific authentication number and a cash card identification number;

processing the transaction; and

transmitting an acknowledgment to a merchant computer of the transaction.

74. The method of claim 73, further comprising the step of:

transmitting the payment code window program to the user, wherein the code window program is used transmit payment information to the server.

75. The method of claim 73, wherein receiving a transaction from a user further comprises the steps of:

creating the payment specific authentication number based on a personal identification number associated with the user and a cash card secret key associated with the cash card.

76. The method of claim 73, wherein processing the transaction further includes:

determining whether an account associated with the cash card is active and contains funds sufficient to purchase the product; and

determining whether the payment specific authentication is correctly computed.

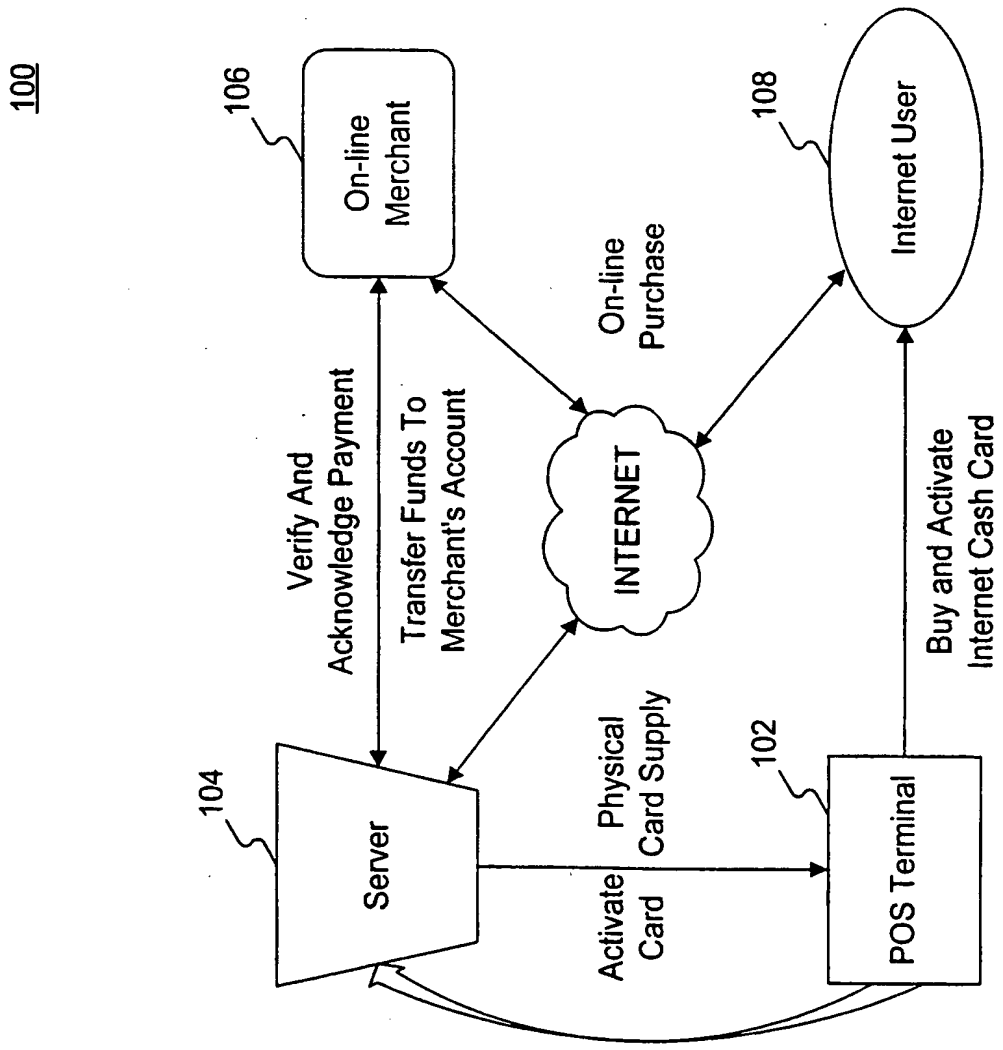

100
106
On-line Merchant
108
Internet User
On-line Purchase
Verify And Acknowledge Payment
Transfer Funds To Merchant's Account
INTERNET
Buy and Activate Internet Cash Card
104
Server
Physical Card Supply
102
POS Terminal
Activate Card

FIGURE 1

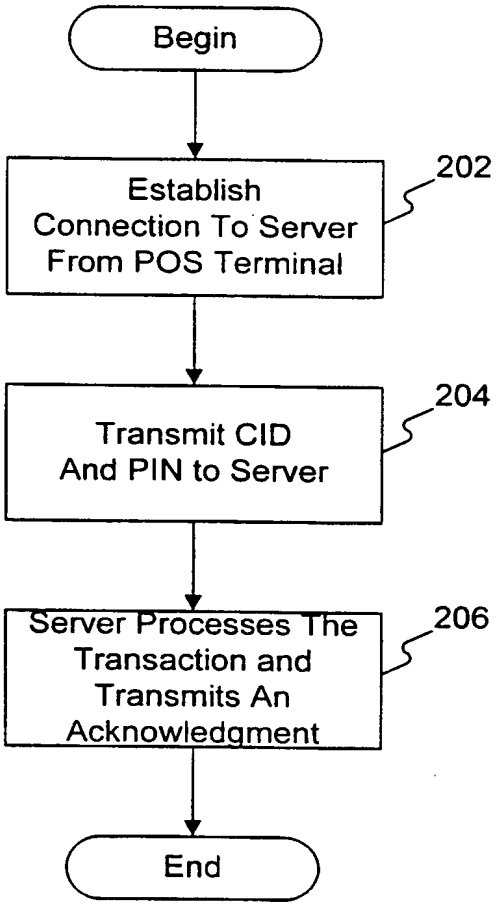


FIGURE 2

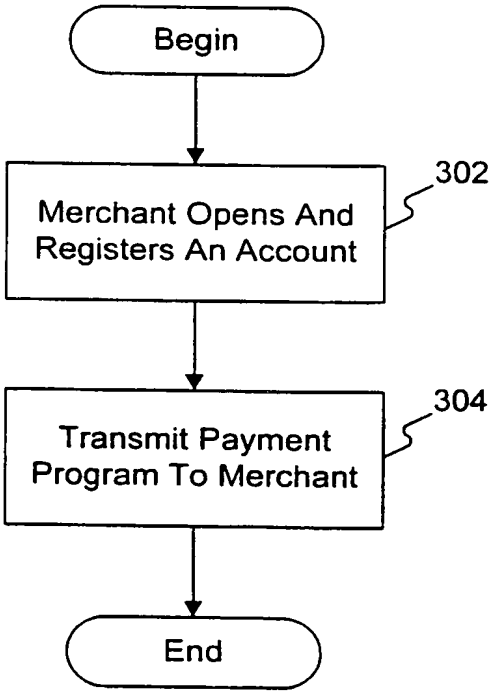

Begin
Merchant Opens And Registers An Account
302
Transmit Payment Program To Merchant
304
End

FIGURE 3

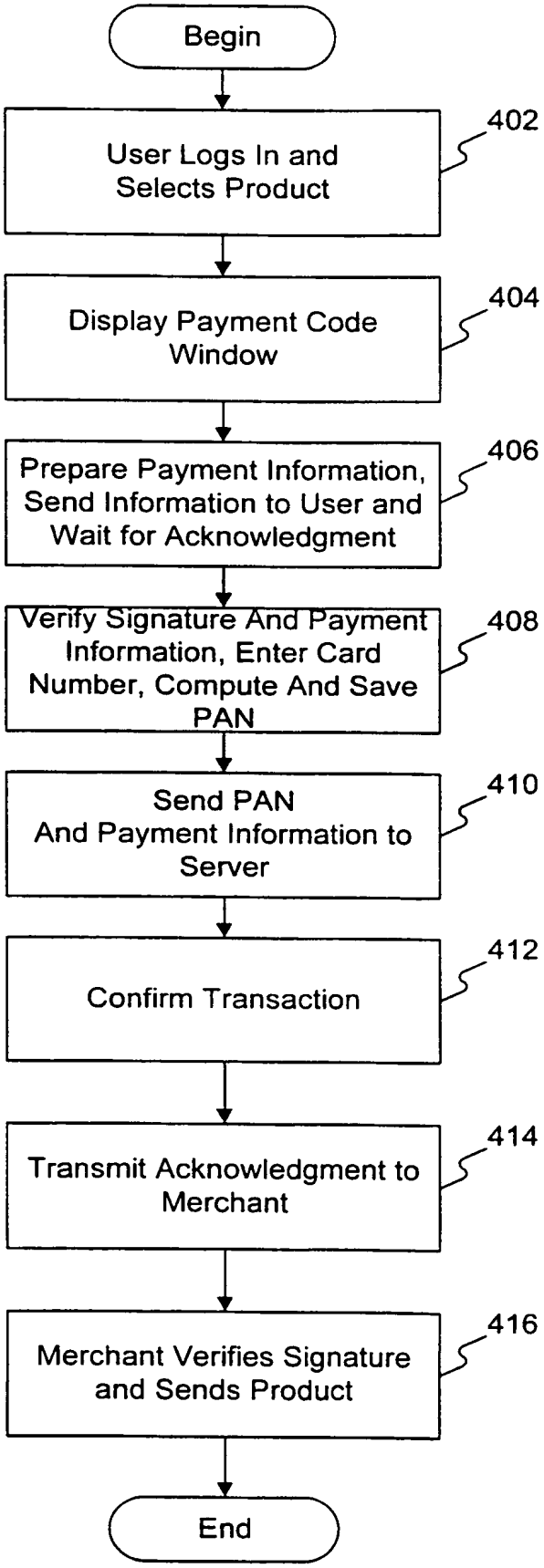


FIGURE 4

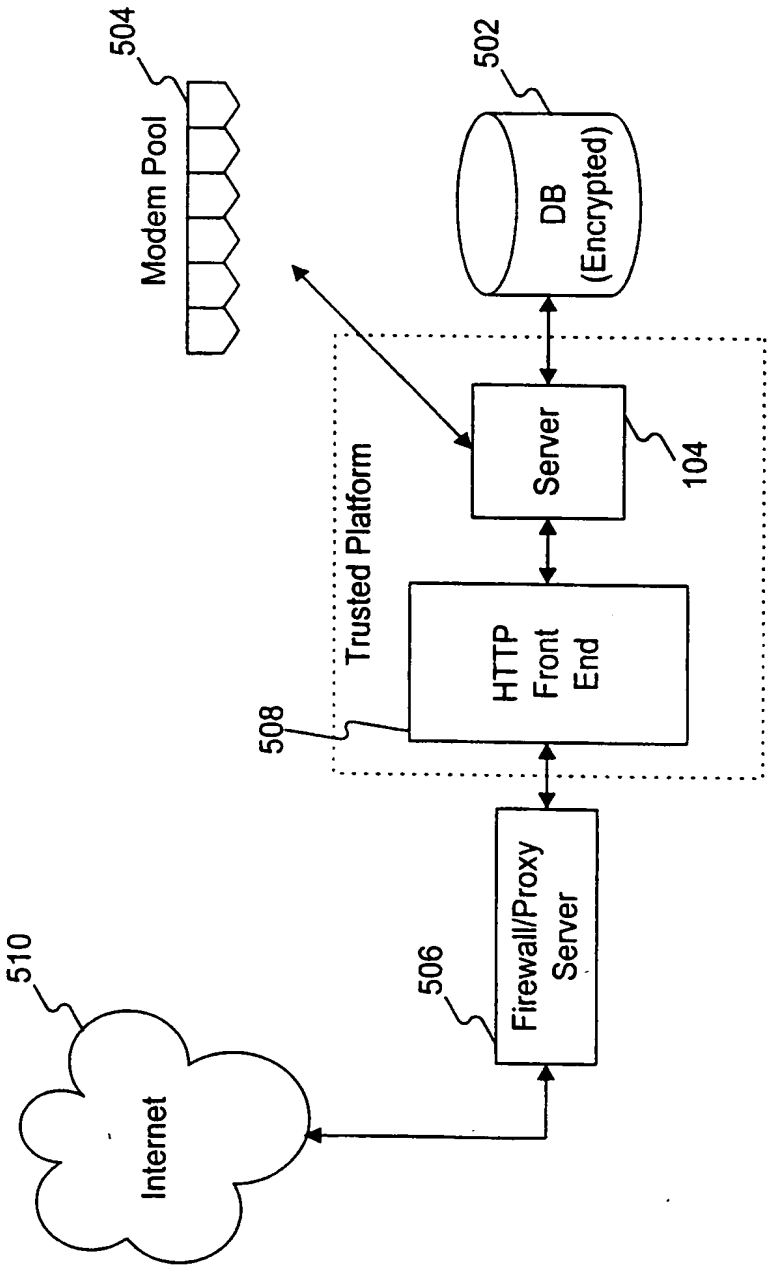

500
504
Modem Pool
502
DB
(Encrypted)
Server
104
Trusted Platform
HTTP
Front
End
508
Firewall/Proxy
Server
506
510
Internet

FIGURE 5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11515 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/14603

(22) International Filing Date: 30 May 2000 (30.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/136,714 28 May 1999 (28.05.1999) US

(71) Applicant: SPENDCASH.COM, INC. [US/US]; Suite 1401, 90 William Street, New York, NY 10038 (US).

(72) Inventors: DOHERTY, Charles, S.; 725 Miller Avenue, #429, Freeport, NY 11520 (US). TSIOUNIS, Yiannis, S.; 81 Greene Street, 2nd Floor, New York, NY 10012 (US).

(74) Agents: GARRETT, Arthur, S. et al.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with declaration under Article 17(2)(a): without abstract; title not checked by the International Searching Authority*

(48) Date of publication of this revised version: 27 June 2002

(15) Information about Correction:
see PCT Gazette No. 26/2002 of 27 June 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR MAKING ANONYMOUS ELECTRONIC PAYMENTS ON THE WORLD WIDE WEB

(57) Abstract:

WO 01/11515 A2

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and Rule 39)

Applicant's or agent's file reference	IMPORTANT DECLARATION	Date of mailing *(day/month/year)*
7932.2-304		30/01/2002
International application No.	International filing date *(day/month/year)*	(Earliest) Priority date *(day/month/year)*
PCT/US 00/ 14603	30/05/2000	28/05/1999
International Patent Classification (IPC) or both national classification and IPC	G06F17/60	
Applicant		
SPENDCASH.COM, INC		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below

1. [X] The subject matter of the international application relates to:
   - a. [ ] scientific theories.
   - b. [ ] mathematical theories
   - c. [ ] plant varieties.
   - d. [ ] animal varieties.
   - e. [ ] essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. [X] schemes, rules or methods of doing business.
   - g. [ ] schemes, rules or methods of performing purely mental acts.
   - h. [ ] schemes, rules or methods of playing games.
   - i. [ ] methods for treatment of the human body by surgery or therapy.
   - j. [ ] methods for treatment of the animal body by surgery or therapy.
   - k. [ ] diagnostic methods practised on the human or animal body.
   - l. [ ] mere presentations of information.
   - m. [ ] computer programs for which this International Searching Authority is not equipped to search prior art.

2. [ ] The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
   [ ] the description [ ] the claims [ ] the drawings

3. [ ] The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:
   [ ] the written form has not been furnished or does not comply with the standard.
   [ ] the computer readable form has not been furnished or does not comply with the standard.

4. Further comments:

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	

Form PCT/ISA/203 (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 203

The claims relate to subject matter excluded from patentability under Art. 52(2) and (3) EPC. Given that the claims are formulated in terms of such subject matter or merely specify commonplace features relating to its technological implementation, the search examiner could not establish any technical problem which might potentially have required an inventive step to overcome. Hence it was not possible to carry out a meaningful search into the state of the art (Rule 45 EPC). See also Guidelines Part B Chapter VIII, 1-6.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.